

THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH  
A residence located at 13 West Lane,  
Rochester, New Hampshire, 03867, to  
include any vehicles and electronic  
devices located within the subject  
premises

Case No. 22-mj-179-01-AJ

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Special Agent Dillon Torno, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND BACKGROUND**

1. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code. I also am a “federal law enforcement officer” within the meaning of Rule 41 of the Federal Rules of Criminal Procedure.

2. I am a Special Agent of the Federal Bureau of Investigation (“FBI”) and have been so employed since October 2012. I am currently assigned to the FBI’s New Hampshire Major Offender Task Force (“NHMOTF”) where I am tasked with investigating violent criminals, gang members, and significant drug traffickers throughout the state. As part of the NHMOTF, I work alongside law enforcement officers from various local, state, and federal agencies throughout the state of New Hampshire.

3. As part of my regular duties as a Special Agent, I investigate criminal violations relating to the distribution of illicit narcotics as specified under Title 21 of the U.S. Code. I have

been trained in drug investigations, narcotic identification, search warrants, undercover techniques, surveillance, debriefing of informants, and other investigative procedures. Through my training, education, and experience, I have become familiar generally with the manner in which drug distribution organizations conduct their illegal activities, including purchasing, manufacturing, storing, and distributing narcotics, the laundering of illegal proceeds, and the efforts of persons involved in such activity to avoid detection by law enforcement. In the course of participating in investigations of drug distribution organizations, I have conducted or participated in surveillance, the purchase of illegal drugs, the execution of search warrants, the use of tracking devices, debriefings of subjects, witnesses, and informants, and reviews of consensually recorded conversations and meetings. I am also familiar with the manner in which narcotics distributors use electronic devices to include cellular telephones and computers to further their illegal activities.

4. Since this affidavit is being submitted for the limited purpose of establishing that probable cause exists to support the issuance of a search warrant, I have not included details about every aspect of the investigation. While this affidavit contains all the material information I am aware of that is pertinent to the requested search warrant, it does not set forth all of my knowledge about this matter.

#### **PURPOSE OF SEARCH WARRANT**

5. This affidavit is made in support of an application for an anticipatory search warrant to search the premises located at 13 West Lane, Rochester, New Hampshire (“the SUBJECT PREMISES”), vehicles (“VEHICLES”) present at the SUBJECT PREMISES, and Electronic Devices (“DEVICES”) present at the SUBJECT PREMISES, as more particularly described in Attachments A and B. Located within the SUBJECT PREMISES, VEHICLES, and on the DEVICES, I seek to seize evidence, fruits, and instrumentalities of the following offenses:

(a) possession with the intent to distribute and the distribution of controlled substances, in violation of Title 21, United States Code, Section 841(a)(1); and (b) conspiracy to possess with the intent to distribute and distribution of controlled substances, in violation of Title 21, United States Code, Section 846, as more particularly described in “Attachment B” hereto.

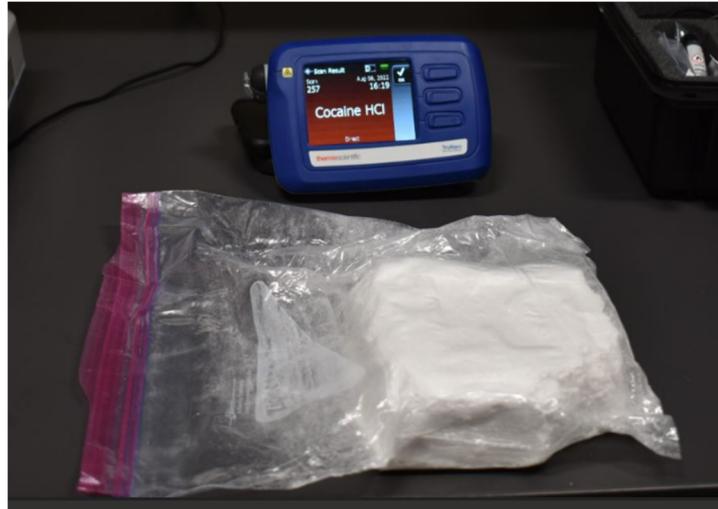
**DESCRIPTION OF PROPERTY TO BE SEIZED**

See Attachment B.

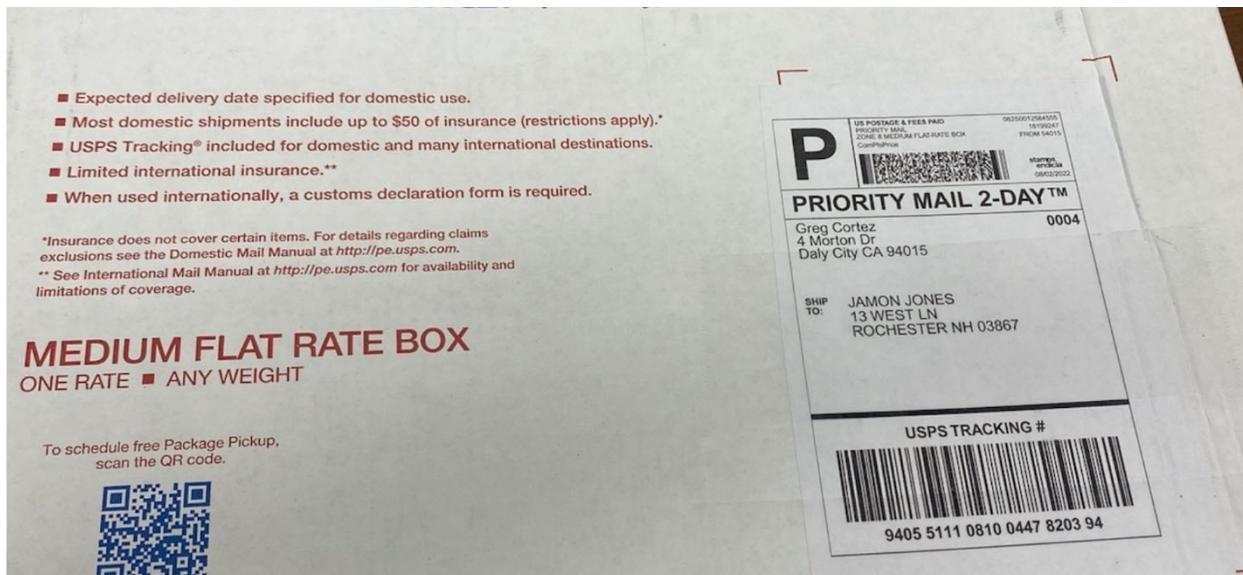
**PROBABLE CAUSE**

6. On August 5, 2022, as part of an ongoing FBI NHMOTF narcotics trafficking investigation, the United States Postal Inspection Service (“USPIS”) seized a package (“SUBJECT PACKAGE”) which is described as a medium Flat Rate Box addressed to Jamon Jones (“JONES”), 13 West Lane, Rochester, New Hampshire, bearing USPS Tracking Number 9405 5111 0810 0447 8203 94, being tracked by phone number [REDACTED] 0425, a phone number known by law enforcement to be used by Jones’ brother, Michael Michaud.

7. The SUBJECT PACKAGE was selected for inspection by USPIS agents, in which K9 “Grimm” from the Manchester, New Hampshire Police Department alerted to the presence of narcotics in the SUBJECT PACKAGE. On August 8, 2022, United Magistrate Judge Andrea K. Johnstone authorized a search of the SUBJECT PACKAGE which resulted in the seizure of a white, square, brick like substance with a “K” stamped into it, that was in a plastic Ziploc bag secreted within multiple layers of vacuum sealed plastic, concealed within in an Express Mail envelope.



8. The SUBJECT PACKAGE is described as a medium Flat Rate Box Priority Mail parcel displaying a computer-generated label and bearing tracking number 9405 5111 0810 0447 8203 94 addressed to "JAMON JONES 13 WEST LN ROCHESTER NH 03867" and bearing a return address of "Greg Cortez 4 Morton Dr Daly City CA 94015". The SUBJECT PACKAGE measures approximately 12"x 3.5"x 14.125" weighs approximately 2 pounds and bears a Priority Mail 2-Day label for which the sender paid \$12.40. The parcel was August 2, 2022, from San Francisco, CA.



9. USPIS agents conducted field tests on the SUBJECT PACKAGE which showed presumptive positive results for the presence cocaine. The total weight of cocaine contained in the Ziploc bag is approximately 511 grams. I know based on my training and experience that 511 grams of cocaine, even with packaging, is a quantity intended for distribution rather than intended for personal use.

10. According to information obtained from a law enforcement database and law enforcement observation, the SUBJECT PREMISES is associated with Jones (date of birth [REDACTED] 1974). Jones has been observed by law enforcement arriving at the SUBJECT PREMISES after the delivery of similarly addressed packages also originating from California.

11. If this application is approved, USPIS and FBI, in conjunction with other state law enforcement agencies, intend to conduct a controlled delivery of a package (“SHAM PACKAGE”) that looks, weighs, and feels like the SUBJECT PACKAGE. The SHAM PACKAGE will have an exact copy of the mailing label and contain a non-narcotic substance similar in appearance to the contents of the SUBJECT PACKAGE.

12. As it relates to firearms, during an interview with law enforcement on August 4, 2022, an FBI Source of Information (“SOI”) stated that Jones purchased a Glock style handgun from Kittery Trading Post approximately three to four months ago, and that it is not unusual for Jones to have this gun on his person or nearby in a vehicle. The SOI stated that they have seen this gun, and that Jones told them that he was looking to buy another gun approximately two months ago.

13. The SOI knows this information because the SOI has been purchasing narcotics from Jones every two to three days for approximately one year. Jones is familiar and friendly with the SOI, and Jones has been inside the SOI’s residence numerous times. The SOI has also

been inside the SUBJECT PREMISES. The SOI also stated that Jones uses his vehicle, a dark colored minivan that looks like a Dodge Grand Caravan, to transport his narcotics and cash. The SOI has been in this vehicle and described a “drug hide” behind the radio, operated by a switch on the driver’s side door. Law enforcement knows this vehicle to be a dark blue Chrysler Town and Country bearing New Hampshire License Plate 5056538, registered to Jones’ brother, Michaud. Law enforcement also knows through physical surveillance of Jones that he uses this minivan on a regular basis in furtherance of his narcotics trafficking .

**TRAINING AND EXPERIENCE OF AFFIANT**

14. Drug trafficking intelligence information has demonstrated that USPS Priority Mail is a method frequently used by drug traffickers for shipping drugs and drug proceeds. Use of Priority Mail is favored because of the speed, reliability, free telephone, and Internet package tracking service, as well as the perceived minimal chance of detection. Priority Mail was originally intended for urgent, business-to-business, correspondence. However, based on law enforcement intelligence and my personal experience with numerous prior packages that were found to contain contraband, packages containing contraband are usually sent from one individual to another individual.

15. Based upon my training, experience, and the training and experience of other agents with whom I have worked and spoken, I know that:

- a. Drug traffickers often store drugs in private places including in their residences, areas of curtilage, outbuildings such as sheds or trailers, vehicles, and in stash houses;
- b. it is common for narcotics traffickers to maintain books, records, receipts, notes, ledgers, airline tickets, receipts relating to the purchase of financial instruments

and or the transfer of funds, and other papers relating to the transportation, ordering, sale and distribution of controlled substances. That the aforementioned books, records, receipts, notes, ledgers, etc., are maintained where the traffickers have ready access to them including their residences and their vehicles;

- c. it is common for drug dealers to secrete contraband, proceeds of drug sales and records of drug transactions in secure locations within their residences, their businesses, their vehicles, stash houses, and/or other locations which they maintain dominion and control over, for ready access and to conceal these items from law enforcement authorities;
- d. Drug traffickers often purchase and/or title their assets in fictitious names, aliases, or the names of relatives, associates, or business entities to avoid detection of these assets by government agencies;
- e. even though these assets are in the names of others, the drug traffickers actually own and continue to use these assets, and exercise dominion and control over them;
- f. it is common for persons involved in drug trafficking to maintain evidence pertaining to their obtaining, secreting, transfer, concealment and/or expenditure of drug proceeds, such as: currency, financial instruments, precious metals and gemstones, electronics, jewelry, books, records, invoices, receipts, records of real estate transactions, bank statements and related records, passbooks, money drafts, letters of credit, money orders, bank drafts, cashiers' checks, bank checks, safe deposit box keys and money wrappers. These items are maintained by the drug traffickers within their residences, businesses, vehicles, or other locations which they maintain dominion and control over;

- g. when drug traffickers amass significant proceeds from the sale of drugs, they often attempt to legitimize these profits through money laundering activities. To accomplish these goals, drug traffickers utilize, among other mechanisms, domestic and international banks and their attendant accounts, casinos, real estate, shell corporations and business fronts, and otherwise legitimate businesses which generate large quantities of currency. Drug traffickers often commingle narcotics proceeds with money generated by legitimate businesses;
- h. Drug traffickers commonly maintain books or papers which reflect names, addresses and/or telephone numbers of their associates in the trafficking organization;
- i. Drug traffickers take or cause to be taken photographs of themselves, their associates, and their property. That these traffickers usually maintain these photographs in their possession;
- j. Drug traffickers often use electronic equipment such as computers, telex machines, facsimile machines, currency counting machines and telephone answering machines to generate, transfer, count, purchase, record and or store information in furtherance of their drug trafficking activities;
- k. Drug traffickers often use cellular and/or portable telephones, smart phones, and other electronic equipment and data storage devices in furtherance of their criminal activities and to maintain contact with associates, drug suppliers and customers;
- l. Drug traffickers who buy and/or sell controlled substances on online marketplaces often rely on one or more means of electronic communication (such as encrypted

email and chat communications) as a means to facilitate this expedient communication.

- m. Drug traffickers who often buy and/or sell controlled substances on online marketplaces often use or take payments in the form of cryptocurrency, money orders or other forms of payments.
- n. Often, drug traffickers possess firearms and other dangerous weapons to protect their profits, supply of drugs, and persons from others who might attempt to forcibly take the traffickers' profits and/or supply of drugs
- o. I know that individuals who distribute narcotics often utilize motor vehicles in order to obtain quantities of controlled substances from their source of supply for distribution. I also know that individuals who are engaged in the distribution of controlled substances utilize motor vehicles in order to transport controlled substances to various locations in order to meet with and distribute controlled substances to potential drug purchasers

16. Based on the above information, I request an anticipatory search warrant for the residence located at the SUBJECT PREMISES as more particularly described in Attachment A and B. I plan to have the SHAM PACKAGE delivered by an undercover agent to that address. It is my intent to execute the search warrant only when the following conditions are met: a) The SHAM PACKAGE is delivered to the SUBJECT PREMISES, and b) a person takes possession of the SHAM PACKAGE and takes it into the SUBJECT PREMISES. The warrant will be executed if, and only if, the SHAM PACKAGE is accepted and taken inside the SUBJECT PREMISES.

17. The following grounds are reasonable cause for allowing the search warrant to be executed during the daytime or in the nighttime: the conditions precedent to executing this warrant may not occur until nighttime. The SHAM PACKAGE may not be taken into the residence until nighttime. In such instance, evidence may be moved or destroyed. Accordingly, I request authorization to execute this warrant in either the daytime or the nighttime.

**Training and Experience on Digital Devices**

18. In addition to documentary evidence of financial and drug trafficking crimes, drug traffickers commonly possess and use multiple cellular telephones simultaneously to conduct their drug trafficking activities and many of these cellular telephones are kept at drug stash houses or at the dealers' own residences. It is common for these cellular telephones to be retained, although not necessarily used, for months or longer by drug traffickers in their vehicles, residences, and businesses. Drug traffickers often do not discard their cellular telephones immediately after they stop actively using them. Therefore, while it is common for drug traffickers to stop using cellular telephones frequently, it is far less common for drug traffickers to discard their cellular telephones after they switch to new cellular telephones. I am aware that collections of cell phones have been found during drug trafficking search warrants of stash houses or residences that have included cell phones that were no longer being used by a particular drug trafficker but had nevertheless been retained.

19. As noted above, evidence of drug crimes can be found in the cell phones and smart phones referenced in the preceding paragraphs. Such evidence can include internet searches for drug-related paraphernalia, addresses, or telephone numbers, as well as incriminating communications via emails, text messages or instant messages. Actions such as

internet searching or emailing (in addition to calling) and text messaging can now be performed from most cell phones. I know, based on my training and experience, that drug traffickers may use encrypted chat platforms like Whatsapp, Textnow, Facebook Messenger, and Instagram, to communicate with people in other countries (often countries from where drugs are brought into the United States) and with people who are most cautious about law enforcement detection. Other applications like Venmo or Cashapp allow people to quickly make financial transfers to others and drug customers may use these methods to pay their sources of supply for drugs.

20. In addition, those involved in drug trafficking crimes commonly communicate using multiple cellular telephones. Contemporaneous possession of multiple cellular telephones is, therefore, evidence of drug trafficking. Moreover, the particular numbers of and the particular numbers dialed by particular cellular telephones can be evidence of drug trafficking. Such numbers can confirm identities of particular speakers and the occurrence of certain events. Based on my training, experience, and information provided by other law enforcement officers, I know that many smartphones can now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

21. As with most electronic/digital technology items, communications made from an electronic device, such as a computer or a cell phone, are often saved or stored on the device. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not

always possible to search digital devices for digital data for a number of reasons, including the following:

- Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.
- Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.
- The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

- Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.

Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

- Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials

contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

- Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment and

can require substantial time. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

22. Based on my training and experience, I believe that it is likely that the SUBJECT PREMISES will contain smartphones that can be unlocked via the use of a fingerprint or facial recognition in lieu of a numeric or alphanumeric password. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of devices such as iPhones and iPads, offer their users the ability to unlock the device via the use of a fingerprint or facial recognition in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID or facial recognition.

23. If a user enables Touch ID or facial recognition on a given device, he or she can register numerous fingerprints or facial profiles that can be used to unlock that device. The user can then use any of the registered fingerprints or facial profiles to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor or by looking into the device's camera. In my training and experience, users of Apple devices that offer Touch ID or facial recognition often enable it because it is considered to be a more convenient way to unlock the device than by entering a passcode, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

24. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID or facial recognition enabled, and a passcode must be used instead, such as: (1) when a certain amount of time has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID or facial recognition recently and the passcode or password has not been entered in the last few days. Thus, in the event law enforcement

encounters a locked Apple device, the opportunity to unlock the device via Touch ID or facial recognition exists only for a short time.

25. Although Apple's Touch ID or facial recognition may be the most common or well-known means for unlocking a device with a fingerprint or facial profile, I am aware that other brands of smartphones like Samsung also offer similar features that work essentially in the same way. Therefore, when I refer to Touch ID or facial recognition I am not just referring to Apple devices, but to similar technology on all smartphones. While I believe that the targets of this investigation likely use smartphones, I am not aware of the particular brand of phone that they use.

26. The passcodes that would unlock the targets' devices is not known to law enforcement. Thus, it may be necessary to press the fingers of the user of the device to the device's Touch ID sensor or put the device's camera in front of the user's face in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock devices with the use of the fingerprints or facial profile of the user is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

27. Based on these facts described above, I believe that there is probable cause to believe that if the SHAM PACKAGE is taken into the SUBJECT PREMISES, the SUBJECT PREMISES, the VEHICLES, and the DEVICES at SUBJECT PREMISES as described in Attachment A and B will contain items described in Attachment B that constitute fruits, evidence or instrumentalities of drug trafficking in violation of Title 21, United States Code, Sections 841(a)(1) (possession with the intent to distribute and distribution of controlled substances) and 846 (conspiracy to possess with the intent to distribute and distribution of controlled substances).

Accordingly, I respectfully request that this Court issue an anticipatory search warrant authorizing the search of the SUBJECT PREMISES, VEHICLES, and DEVICES for the items described in Attachment B, upon the occurrence of the triggering events described above. I also respectfully request this warrant to authorize an image and forensic search of any DEVICES seized.

/s/ Dillon Torno  
SPECIAL AGENT DILLON TORNO  
FEDERAL BUREAU OF INVESTIGATION

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: Aug 9, 2022

Time: 1:35 PM, Aug 9, 2022

/s/ Andrea K. Johnstone

Hon. Andrea K. Johnstone  
United States Magistrate Judge

**ATTACHMENT A**

(Description of Property to be Searched)

13 West Lane, Rochester, New Hampshire, 03867 is a white mobile trailer style home, with black trim. The home has a front door accessed from a wooden porch, and a rear door. The driveway is located on the front right side of the home with a white mailbox on a post, marked with 13, to the right of the driveway and to the left of a mailbox marked 9.



**ATTACHMENT B**

(Particular Things to be Seized)

- The SHAM PACKAGE which is a USPS Medium Flat Rate box bearing USPS Tracking Number 9405 5111 0810 0447 8203 94.
- Books, records, receipts, notes, and ledgers relating to the ordering, receipt, possession, transportation, purchasing, shipment, tracking, delivery and distribution of controlled substances
- Papers and records relating to names, addresses, and telephone numbers relating to co-conspirators, sources of drug supply, and drug customers
- Indicia of occupancy, residency, and ownership or use of the subject premises, including, but not limited to, utility and telephone bills, cancelled envelopes, rental, purchase or lease agreements, identification documents and keys
- Electronic devices to include but not limited to cellular telephones, computers, tablets, and the memory thereof. Such devices may be imaged and searched on site or elsewhere without further order of the Court
- Controlled substances and drug paraphernalia, including, chemical diluents, weighing scales, and items utilized in the packaging of controlled substances
- U.S. currency, cryptocurrency, or any and all monetary instruments, or other items of value used in, or intended for use in, or derived from trafficking in controlled substances
- Weapons to include handguns, ammunition, rifles, shotguns, hand crafted guns, explosive devices, etc., in which there is no immediate appearance of legitimate use and of which may be used in conjunction with the distribution of controlled substances

All of which constitute fruits, evidence and/or instrumentalities of violations of Title 21, United States Code, Sections 841 and 846.